UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,640	03/13/2001	Laura Painton Swiler	SD6528S93789	2888

20567 7590 09/23/2004

SANDIA CORPORATION
P O BOX 5800
MS-0161
ALBUQUERQUE, NM 87185-0161

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/805,640	SWILER ET AL.	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-24 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-24 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 13 March 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3/13/01.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ortalo et al (Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security) in view of Clarkson (Approximation Algorithms for Shortest Path Motion Planning).

With respect to Claim 1, Ortalo et al meets the limitation of "describing a set of potential attacks on the computer system through which a change in status of the computer system could be effected, wherein the change comprises a transition from a start condition to an end condition which is different from the start condition" on page 635, column 1, paragraph 4, last sentence and on page 636, column 1, paragraph 2, first sentence; and "defining a set of paths comprising at least one path for each potential attack described, wherein each path comprises at least one event necessary for transition from the start condition to the end condition, which transition can include passage through intermediate conditions in transit from the start condition to the end condition" on page 636, column 1, paragraph 3; and "for each path in said set of paths, assigning a length value, L, corresponding to a metric reflecting at least one security significant condition bearing on likelihood of success of an attacker attempting to effect said transition from the start condition, through intermediate conditions, if any, to the end condition, so that the value of L correlates inversely with said likelihood of success" on page 636, column 1, paragraph 1, last

two sentences. The shortest path inherently refers to the length of the shortest path. The shorter the length, the less the effort needed by an attacker to effect transition to the next attack state.

Ortaló et al meets the limitation of "identifying within said set of paths at least one shortest path defined as that having the smallest length value of paths in the set of paths" on page 636, column 1, paragraph 1, second to the last sentence. The shortest path is inherently the smallest length of paths. Ortalo et al however does not meet the following limitation.

The limitation of "identifying, from within the set of paths, specific paths (denoted "epsilon optimal paths") having a length, $L \leq (1+\epsilon)$ times the length of the shortest path, where ϵ is a non-negative number that accounts for uncertainty in individual edge metrics and uncertainty in the actual path the attacker will choose; and designating "epsilon optimal paths" as high risk attack paths" is met by Clarkson on page 56, column 1. A path within $(1+\epsilon)$ of the shortest length is equivalent to $L \leq (1+\epsilon)$ times the length of the shortest path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Clarkson within the system of Ortalo et al because determining the shortest path length from the attacker to the target system allows the least effort network vulnerabilities to be determined and patched so as to harden the network and prevent future similar attacks.

With respect to Claim 2, Ortalo et al meets the limitation of "wherein the at least one security significant condition is selected from the group consisting of estimated time necessary for the attacker to achieve said success, estimated cost to the attacker in order to achieve said success, estimated degree of effort by the attacker in order to achieve said success, estimated

likelihood of detection of the attacker's efforts in attempting to achieve said success, estimated likelihood of approbation of an attack, and any combination thereof" is met on page 635, column 1, last paragraph, last sentence and on column 2, first and second paragraphs.

With respect to Claim 3, Ortalo et al meets the limitation of "the step of generating a graphical depiction of at least a portion of the set of paths, wherein, for each path, nodes represent discrete physical states of the computer system and edges adjoining nodes represent transitions between physical states in the computer system" on Fig. 1 and on page 635, column 1, paragraph 3.

With respect to Claim 4, Ortalo et al meets the limitation of "wherein nodes shown in the graphical depiction include a physical state associated with the start condition, a physical state associated with the end condition, and physical states associated with intermediate conditions, if any exist for a given path" on Fig. 1 and on page 635, column 1, paragraph 3.

With respect to Claim 5, Ortalo et al meets the limitation of "wherein redundant paths to nodes are eliminated, by enforcing an ordering on acquisition of multiple, independent vulnerabilities in the graph" on page 636, column 1, paragraph 2 and on page 637, column 1, paragraph 5, last sentence.

With respect to Claim 6, Ortalo et al meets the limitation of "wherein transitions between physical states in the computer system are characterized mathematically by assigning each

transition an edge weight based on at least one security significant metric having an assigned value" on Fig. 1 and 2.

With respect to Claim 7, Ortalo et al meets the limitation of "wherein the assigned value of the at least one security significant metric is calculated as a function of an element capable of affecting security of the computer system, wherein the element is selected from the group consisting of capabilities of at least one hypothesized attacker and, network configuration information" on page 636 on column 1, paragraph 1-3.

With respect to Claim 8, Ortalo et al meets the limitation of "hypothesized probability of success of the attacker in effecting a given transition between physical states; hypothesized cost to the attacker in effecting a given transition between physical states; hypothesized level of effort of the attacker in effecting a given transition between physical states hypothesized length of time necessary for the attacker to succeed in effecting a given transition between physical states; and any combination thereof" on page 635, column 1, last paragraph, last sentence and on column 2, first and second paragraphs.

With respect to Claim 9, Ortalo et al meets the limitation of "providing at least one configuration file from which is obtained the information about the network and machine configuration of the computer system" on page 636, paragraph two; and "providing at least one attack template comprising hypothesized attack information which, in turn, comprises at least one attack step which, if successful, could effect a change in status of the computer system given

its configuration" on Fig. 1 and on page 636, column 1, paragraph 2; and "providing at least the attacker profile comprising hypothesized attacker information which, in turn, comprises at least one capability of at least one hypothesized attacker, which, if exercised, could enable said at least one attack step to take place successfully" on page 636, column 1, paragraph 3.

With respect to Claim 10, Ortalo et al meets the limitation of "wherein the configuration file is generated as a result of gathering information about the network configuration by polling machines to obtain data about physical elements comprising the system" on page 635, column 1, paragraph 2.

With respect to Claim 11, Ortalo et al meets the limitation of "wherein the physical elements comprising the system are selected from the group consisting of IP address, machine type, operating system, users, file system structure, vulnerabilities on machines, and programs running on machines" on page 635, column 1, paragraph 2.

With respect to Claim 12, Ortalo et al meets the limitation of "a processing unit; a storage system connected with the processing unit; an input device connected with the processing unit; an output device connected with the processing unit" on page 635, column 1, paragraph 3. The nodes represent computer systems that inherently have these components. Ortalo et al meets the limitation of "potential attack set input means for using the input device to load a set of potential attacks into the storage system, wherein the set of potential attacks define attacks through which a change in status of the computer system could be effected, wherein the change comprises a

transition from a start condition to an end condition which is different from the start condition" on page 635, column 1, paragraph 4, last sentence and on page 636, column 1, paragraph 2, first sentence; and "path set definition means for defining a set of paths comprising at least one path for each attack in the set of potential attacks, wherein each path comprises at least one event necessary for transition from the start condition to the end condition, which transition can include passage through intermediate conditions in transit from the start condition to the end condition" on page 636, column 1, paragraph 3; and "length value assigning means for assigning, for each path in the set of paths, a length value, L, corresponding to a metric reflecting at least one security significant condition bearing on likelihood of success of an attacker attempting to effect said transition from the start condition, through intermediate conditions, if any, to the end condition, so that the value of L correlates inversely with said likelihood of success" on page 636, column 1, paragraph 1, last sentence; and "shortest path identification means for identifying within said set of paths at least one shortest path defined as that having the smallest length value of paths in the set of paths" on page 636, column 1, paragraph 1, second to last sentence. The presence of these process steps in the prior art obviate the existence of hardware means that implement these processes. Ortalo however does not meet the following limitation.

The limitation of "epsilon optimal path identification means for identifying, from within the set of paths, specific paths (denoted "epsilon optimal paths') having a length, $L \leq (1+ \epsilon)$ times the length of the shortest path, where ϵ is a non-negative number that accounts for uncertainty in individual edge metrics and uncertainty in the actual path the attacker will choose; and output means for using the output device to communicate "epsilon optimal paths" to a user" is met by Clarkson on page 56, column 1.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Clarkson within the system of Ortalo et al because determining the shortest path length from the attacker to the target system allows the least effort network vulnerabilities to be determined and patched so as to harden the network and prevent future similar attacks.

With respect to Claim 13, its limitation is similar to Claim 2 limitation and hence its rejection can be found therein.

With respect to Claim 14, its limitation is similar to Claim 3 limitation and hence its rejection can be found therein.

With respect to Claim 15, its limitation is similar to Claim 4 limitation and hence its rejection can be found therein.

With respect to Claim 16, its limitation is similar to Claim 5 limitation and hence its rejection can be found therein.

With respect to Claim 17, its limitation is similar to Claim 6 limitation and hence its rejection can be found therein.

With respect to Claim 18, its limitation is similar to Claim 7 limitation and hence its rejection can be found therein.

With respect to Claim 19, its limitation is similar to Claim 8 limitation and hence its rejection can be found therein.

With respect to Claim 20, Ortalo et al meets the limitation of "configuration file input means for using the input device to load at least one configuration file from which is obtained the information about the network and machine configuration of the computer system" on page 636, paragraph 2.

With respect to Claim 21, Ortalo et al meets the limitation of "attack template input means for using the input device to load at least one attack template comprising hypothesized attack information which, in turn, comprises at least one attack step which, if successful, could effect a change in status of the computer system given its configuration" on Fig. 1 and on page 636, column 1, paragraph 2.

With respect to Claim 22, Ortalo et al meets the limitation of "attacker profile input means for using the input device to load at least one attacker profile comprising hypothesized attacker information which, in turn, comprises at least one capability of at least on hypothesized attacker, which, if exercised, could enable said at least one attack step to take place successfully" on page 636, column 1, paragraph 3.

With respect to Claim 23, its limitation is similar to claim 10 limitation and hence its rejection can be found therein.

With respect to Claim 24, its limitation is similar to claim 11 limitation and hence its rejection can be found therein.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Please note the Patent Office will be moving to the Alexandria campus next month. The new phone number for myself, Tracey Akpati is (571) 272-3846, my SPE, Kim Vu is (571) 272-3859 and the receptionist is (571) 272-2100.

OTA

AU 2135